Dictamen 5/2020 sobre el proyecto de decisión de la autoridad de control competente de Luxemburgo en relación con la aprobación de los requisitos de acreditación de un organismo de certificación con arreglo al artículo 43.3 del RGPD

Adoptado el 29 de enero de 2020

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Índice

El Comité Europeo de Protección de Datos

Vistos el artículo 63, el artículo 64, apartado 1, letra c), incisos 3 a 8, y el artículo 43, apartado 3, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en lo sucesivo, el «RGPD»),

Visto el artículo 51, apartado 1, letra b) de la Directiva (UE) 2016/680 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (en lo sucesivo, la «Directiva sobre la policía»),

Visto el Acuerdo sobre el Espacio Económico Europeo y, en particular, su anexo XI y su Protocolo 37, modificado por la Decisión del Comité conjunto del EEE n.º 154/2018, de 6 de julio de 2018,[1]

Vistos los artículos 10 y 22 de su Reglamento interno, de 25 de mayo de 2018,

Considerando lo siguiente:

(1) La principal función del Comité es velar por la aplicación coherente del Reglamento 2016/679 (en lo sucesivo, el «RGPD») en todo el Espacio Económico Europeo. De conformidad con el artículo 64, apartado 1, del RGPD, el Comité emitirá un dictamen cuando una autoridad de control (AC) tenga la intención de aprobar los requisitos de acreditación de organismos de certificación con arreglo al artículo 43. El objetivo del presente dictamen es, por tanto, crear un enfoque armonizado en relación con los requisitos que aplicará una autoridad de control para la protección de datos o el organismo nacional de acreditación para la acreditación de un organismo de certificación. Aunque el RGPD no impone un único conjunto de requisitos para la acreditación, sí promueve la coherencia. El Comité pretende alcanzar este objetivo en sus dictámenes, en primer lugar, animando a las autoridades de control a elaborar sus requisitos para la acreditación con arreglo a la estructura establecida en el anexo de las Directrices del Comité Europeo de Protección de Datos (CEPD) sobre acreditación de organismos de certificación, y, en segundo lugar, analizándolos mediante un modelo proporcionado por el CEPD que permite la evaluación comparativa de los requisitos (con arreglo a la norma ISO 17065 y a las directrices del CEPD sobre la acreditación de los organismos de certificación).

(2) Con referencia al artículo 43 del RGPD, las autoridades de control competentes adoptarán requisitos de acreditación. No obstante, aplicarán el mecanismo de coherencia a fin de permitir que se genere confianza en el mecanismo de certificación, en particular mediante el establecimiento de un alto nivel de requisitos.

(3) Si bien los requisitos de acreditación están sujetos al mecanismo de coherencia, no significa que los requisitos deban ser idénticos. Las autoridades de control competentes disponen de un margen de discrecionalidad en lo que respecta al contexto nacional o regional, y deberán tener en cuenta su normativa nacional. El objetivo del dictamen del CEPD no es conseguir un conjunto único de requisitos

[1] Las referencias a la «Unión» realizadas en el presente dictamen deben entenderse como referencias al «EEE».

de la UE, sino evitar incoherencias significativas que puedan afectar, por ejemplo, a la confianza en la independencia o el conocimiento de los organismos de certificación acreditados.

(4) Las «Directrices 4/2018 sobre la acreditación de los organismos de certificación en virtud del artículo 43 del Reglamento general de protección de datos (2016/679)» (en lo sucesivo, las «Directrices») y las «Directrices 1/2018 sobre la certificación e identificación de los criterios de certificación de acuerdo con los artículos 42 y 43 del Reglamento (CE) n.º 2016/679» servirán como hilo conductor en el contexto del mecanismo de coherencia.

(5) Si un Estado miembro estipula que los organismos de certificación deben estar acreditados por la autoridad de control, esta deberá establecer requisitos de acreditación, incluidos, entre otros, los requisitos enumerados en el artículo 43, apartado 2. En comparación con las obligaciones relativas a la acreditación de los organismos de certificación por parte de los organismos nacionales de acreditación, el artículo 43 ofrece menos información sobre los requisitos de acreditación cuando es la propia autoridad de control la que lleva a cabo la acreditación. Para contribuir a la adopción de un enfoque armonizado de la acreditación, los criterios de acreditación utilizados por la autoridad de control deben guiarse por la norma ISO/IEC 17065 y complementarse con los requisitos adicionales que establezca la autoridad de control de conformidad con el artículo 43, apartado 1, letra b). El CEPD señala que el artículo 43, apartado 2, letras a) a e), refleja y especifica los requisitos de la norma ISO 17065, lo que contribuirá a la coherencia[2].

(6) En virtud del artículo 64, apartado 1, letra c) y los apartados 3 y 8 del RGPD, en combinación con el artículo 10, apartado 2, del Reglamento interno del CEPD, el dictamen del Comité deberá adoptarse en un plazo de ocho semanas a contar desde el primer día hábil posterior al momento en que el presidente y la autoridad de control competente hayan decidido que el expediente está completo. Por decisión del presidente, dicho plazo podrá ampliarse otras seis semanas teniendo en cuenta la complejidad del asunto.

HA ADOPTADO EL SIGUIENTE DICTAMEN:

1 RESUMEN DE LOS HECHOS

1. La autoridad de control de Luxemburgo (AC LU) ha presentado al CEPD su proyecto de requisitos de acreditación con arreglo al artículo 43, apartado 1, letra a). Tras una decisión por la que se considera el expediente completo, se emitió el 25 de octubre de 2019. La AC LU llevará a cabo acreditaciones de los organismos de certificación para certificar la utilización de criterios de certificación del RGPD.
2. De conformidad con el artículo 10, apartado 2, del Reglamento interno del Comité, debido a la complejidad del asunto en cuestión, el presidente decidió prorrogar otras seis semanas el período de adopción inicial de ocho semanas.

[2] Apartado 39 de las Directrices: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf

2 EVALUACIÓN

2.1 Razonamiento general del CEPD sobre el proyecto de requisitos de acreditación presentado

El objetivo del presente dictamen es evaluar los requisitos de acreditación elaborados por una AC, ya sea además de la norma ISO 17065 o como un conjunto completo de requisitos, a fin de permitir a un organismo nacional de acreditación o a una AC, de conformidad con el artículo 43, apartado 1, del RGPD, acreditar un organismo de certificación responsable de la expedición y renovación de la certificación, de conformidad con el artículo 42 del RGPD. Esto se entiende sin perjuicio de las funciones y competencias de la AC competente. En este caso concreto, el Comité señala que la legislación nacional encomienda a la AC LU la acreditación de los organismos de certificación. A este fin, la AC LU ha desarrollado una serie de requisitos específicos para la acreditación de los organismos de certificación, junto con una serie de criterios de certificación que aún no se han aprobado formalmente.

La evaluación de los requisitos de acreditación tiene por objeto examinar las variaciones (adiciones o supresiones) de las Directrices y, en particular, del anexo. Además, el dictamen del CEPD también se centra en todos los aspectos que pueden afectar a un enfoque coherente en relación con la acreditación de los organismos de certificación.

Cabe señalar que el objetivo de las directrices sobre la acreditación de los organismos de certificación es ayudar a las AC a definir sus requisitos de acreditación. Las directrices que figuran en el anexo no constituyen requisitos de acreditación como tales. Por lo tanto, los requisitos de acreditación para los organismos de certificación deben ser definidos por la AC de manera tal que permita su aplicación práctica y coherente, como requiere el contexto de la AC.

El Comité ha llevado a cabo su evaluación en consonancia con la estructura prevista en el anexo 1 de las Directrices. Cuando el dictamen no se pronuncie sobre una sección específica de los proyectos de requisitos de acreditación de la AC LU, debe entenderse que el Comité no formula ninguna observación y no pide a la AC LU que tome nuevas medidas. El Comité señala que la AC LU ha proporcionado información para ayudar a evaluar los proyectos de requisitos de acreditación. No obstante, el dictamen del Comité solo aborda el proyecto de requisitos de acreditación.

Además, el presente dictamen no refleja los elementos presentados por la AC LU que no entran en el ámbito de aplicación del artículo 43, apartado 2, del RGPD, como las referencias a la legislación nacional. No obstante, el Comité observa que la legislación nacional debe estar en consonancia con el RGPD, cuando sea necesario.

2.2 Principales puntos de interés para la evaluación (artículo 43.2 del RGPD y anexo 1 de las directrices del CEPD) proporcionados por los requisitos de acreditación para la evaluación coherente de los siguientes puntos:

a. abordar todos los ámbitos clave que figuran en el anexo de las Directrices y considerar toda desviación del anexo;

b. independencia del órgano de certificación;

c. conflictos de intereses del organismo de certificación;

d. conocimientos técnicos del organismo de certificación;

e. salvaguardias adecuadas para garantizar que el organismo de certificación aplique los criterios de certificación del RGPD adecuadamente;

f. procedimientos para la expedición, revisión periódica y retirada de la certificación del RGPD; y

g. tramitación transparente de las reclamaciones sobre infracciones de la certificación.

3. Considerando que:

a. el artículo 43, apartado 2, del RGPD proporciona una lista de áreas de acreditación que un organismo de certificación debe abordar para ser acreditado,

b. el artículo 43, apartado 3, del RGPD establece que los requisitos para la acreditación de los organismos de certificación serán aprobados por la autoridad de control competente,

c. el artículo 57, apartado 1, letras p) y g), del RGPD establece que una autoridad de control competente debe elaborar y publicar los criterios para la acreditación de organismos de certificación y puede decidir llevar a cabo ella misma la acreditación de dichos organismos de certificación,

d. el artículo 64, apartado 1, letra c), del RGPD establece que el Comité emitirá un dictamen cuando una autoridad de control tenga la intención de aprobar los requisitos de acreditación para un organismo de certificación con arreglo al artículo 43, apartado 3,

el Comité considera lo siguiente:

2.2.1 OBSERVACIONES GENERALES

4. El Comité observa que los proyectos de requisitos de acreditación no siguen completamente la estructura establecida en el anexo 1 de las Directrices. Faltan, por ejemplo, las secciones «ámbito de aplicación» y «términos y definiciones». En relación con esto, el Comité señala que algunos términos no se utilizan de forma coherente en todo el documento, como «cliente» y «solicitante». Para evitar confusiones, los términos empleados deben ajustarse a las Directrices y a las definiciones del anexo cuando sea posible, y utilizarse de manera coherente. Por consiguiente, con el fin de facilitar la evaluación, el Comité anima a la AC LU a que siga la estructura del anexo 1 [de las Directrices] en el proyecto de requisitos de acreditación y añada las secciones que faltan.

5. El Comité observa que, a lo largo de todo el documento, hay varias referencias a los requisitos «del presente mecanismo de certificación» (por ejemplo, el requisito 4.6.4) o a los organismos de certificación que están acreditados «en virtud del mecanismo de certificación (...)» (por ejemplo, el requisito 2.2.2). La referencia al mecanismo de certificación parece ser un problema de redacción. Así pues, el Comité anima a LU SA a que vuelva a redactar las referencias para reflejar que los organismos de certificación están acreditados según los requisitos aprobados por la autoridad de control.

6. En una nota similar, la referencia a los «requisitos establecidos en este mecanismo de certificación», utilizada en todo el documento (por ejemplo, el requisito 1.1.1.2), es confusa. Una referencia más apropiada podría ser «los criterios establecidos en el mecanismo de certificación». Así pues, el Comité anima a la AC LU a aclarar todas las referencias al «mecanismo de certificación» que aparecen a lo largo del documento.

7. El Comité observa que varios requisitos (por ejemplo, 3.2.1.1 y 4.1.2) se refieren a las «normas internacionales pertinentes», la «norma pertinente» o la «norma especificada». Sin embargo, no existe una definición de dichas normas y, por lo tanto, no está claro cuáles son las normas mencionadas. Por lo tanto, el Comité recomienda a la AC LU que aclare el significado de dichas normas. Esto podría hacerse, por ejemplo, en las secciones «ámbito de aplicación» o «términos y definiciones».

2.2.2 REQUISITOS GENERALES DE ACREDITACIÓN

8. El Comité señala que el requisito de la AC LU 1.1.1.1 se refiere a otra norma, la «ISAE 3000», que el CEPD no ha evaluado. Por lo tanto, el Comité recomienda a la AC LU que aclare que los requisitos no se pueden anular por ninguna norma externa, como ISAE 3000.

9. El Comité observa que los requisitos de 1.6 no incluyen la obligación del organismo de certificación de publicar y poner a disposición del público todas las versiones de los criterios aprobados y todos los procedimientos de certificación, según lo establecido en el anexo de las Directrices (sección 4.6). El Comité señala que la AC LU podría ser el titular del régimen de certificación; sin embargo, el Comité considera que sería útil añadir una referencia adecuada para garantizar que los criterios estén actualizados y sean fácilmente accesibles a través del propio organismo de certificación. A este respecto, el Comité considera que, al poner a disposición la información únicamente previa solicitud, tal como se establece en el requisito 1.6.1, la AC LU establece un requisito más estricto que el anexo, que establece que la información deberá ser fácilmente accesible al público. Por lo tanto, el Comité recomienda a la AC LU que modifique el requisito para incluir la obligación del organismo de certificación de asegurarse de que todas las versiones de los criterios aprobados y todos los procedimientos de certificación sean fácilmente accesibles al público, de conformidad con el anexo de las Directrices.

10. El Comité señala que el requisito 1.2.4 se refiere al «proceso certificado». El Comité considera que podrían utilizarse términos más precisos, en consonancia con las Directrices, como «operaciones/actividades de tratamiento certificadas». Esto proporciona un ámbito de certificación más amplio, según lo previsto en el RGPD. Por lo tanto, el Comité recomienda a la AC LU que modifique el proyecto de requisitos en consecuencia.

2.2.3 REQUISITOS EN MATERIA DE RECURSOS

11. El Comité señala que el requisito 3.1.1.2 parece repetitivo y poco claro, y que la distinta terminología no ayuda. Por ejemplo, el párrafo tercero reza como si el socio participante en el contrato tomase la decisión de idoneidad basándose únicamente en su juicio. El Comité recomienda que AC LU vuelva a redactar el texto para que el requisito resulte más claro y comprensible, utilizando una terminología coherente.

2.2.4 REQUISITOS DEL PROCESO

12. El Comité observa que el requisito 4.2.1 ofrece varios ejemplos de información necesaria. No obstante, los dos primeros ejemplos proporcionados deben constituir un requisito por sí mismos, de conformidad con la sección 7.2 del anexo 1 de las Directrices. Por lo tanto, el Comité anima a la AC LU a modificar la redacción e incluir los ejemplos anteriormente mencionados como requisitos.

13. Con respecto a la sección 4.4 (Evaluación) de los requisitos de acreditación de la AC LU, el Comité considera que los requisitos de acreditación deben incluir la obligación del organismo de certificación de garantizar que se apliquen métodos de evaluación y que dichos métodos de evaluación, descritos en el mecanismo de certificación, estén normalizados y sean de aplicación general. Esto garantizaría la utilización de métodos de evaluación comparables para objetivos de evaluación comparables. El

organismo de certificación deberá justificar cualquier desviación respecto a estos métodos de evaluación. Por lo tanto, el Comité recomienda a la AC LU que modifique el proyecto a fin de incluir la obligación antes mencionada para el organismo de certificación.

14. Además, el Comité toma nota de que el requisito 4.4.2 establece que, aunque no se permita la externalización, el organismo de certificación puede recurrir a expertos externos para ámbitos específicos. A este respecto, es importante aclarar que el organismo de certificación seguirá siendo responsable de la toma de decisiones, incluso cuando recurre a expertos externos. Por lo tanto, el Comité recomienda a la AC LU que modifique la redacción en el requisito 4.4.2 en consecuencia.

15. El Comité observa que la sección 4.7 de los requisitos de acreditación de la AC LU («documentación de certificación») no aborda el requisito del anexo para documentar el período de supervisión (sección 7.9). Por lo tanto, el Comité anima a la AC LU a incluir el período de seguimiento en el sentido de la sección 7.9 sobre la supervisión.

16. Por lo que se refiere a la sección 4.8 («Lista de actividades de tratamiento certificadas») de los requisitos de acreditación de la AC LU, el requisito 4.8.1 establece que la información se facilitará al público «previa solicitud». El Comité opina que la obligación de transparencia establecida en la sección 7.8 del anexo 1 se cumpliría mejor si el organismo de certificación hubiera puesto a disposición la información de manera proactiva. Así pues, el Comité recomienda a la AC LU, que modifique el proyecto para que el organismo de certificación haga pública la información mencionada en la sección 7.8 del anexo 1 de las Directrices.

17. El Comité observa que la sección 4.8 contiene un epígrafe sobre supervisión sin ningún requisito. El Comité recomienda que la AC LU aclare cómo se llevará a cabo el seguimiento.

18. En cuanto a la resolución, reducción, suspensión o retirada de la certificación (subsección 4.10), el Comité señala que no se hace referencia a la obligación del organismo de certificación de aceptar decisiones y órdenes de la autoridad de control competente de retirar o no expedir certificados a un cliente (solicitante) si no se cumplen o han dejado de cumplirse los requisitos para la certificación. Esta obligación se establece en el artículo 58, apartado 2, letra h), del RGPD y en la sección 7.11 del anexo 1. Por lo tanto, el Comité recomienda a la AC LU que modifique los requisitos de acreditación en los que se especifican las normas relativas a la retirada, resolución, reducción o suspensión de la certificación.

19. El Comité observa que la sección 9 del anexo que contiene epígrafes generales no tiene requisitos. Por ejemplo, el apartado 9.3.4, relativo a la suspensión o retirada de la acreditación, no se incluye aquí. Se trata de epígrafes significativos que justifican la adición de referencias cruzadas a las secciones o requisitos pertinentes. El Comité anima a la AC LU a que aclare dónde se especifican los requisitos.

3 CONCLUSIONES Y RECOMENDACIONES

20. El proyecto de requisitos de acreditación de la autoridad de control de Luxemburgo puede dar lugar a una aplicación incoherente de la acreditación de los organismos de certificación, y deben realizarse los siguientes cambios:

21. Como observación general, el Comité recomienda a la AC LU que:

1. aclare el significado de «norma», como se menciona en varios requisitos (por ejemplo, 3.2.1.1 y 4.1.2). Esto podría hacerse, por ejemplo, en las secciones «ámbito de aplicación» o «términos y definiciones».

22. En cuanto a los «requisitos generales de acreditación», el Comité recomienda a la AC LU que:

    1. aclare que los requisitos no se pueden anular por ninguna norma externa, como ISAE 3000.

    2. modifique los requisitos en la sección 1.6 para incluir la obligación del organismo de certificación de publicar todas las versiones de los criterios aprobados y todos los procedimientos de certificación y asegurarse de que sean fácilmente accesibles al público, de conformidad con el anexo de las Directrices.

23. En cuanto a los «requisitos en materia de recursos», el Comité recomienda a la AC LU que:

    1. reformule el requisito 3.1.1.2 para que sea más claro y comprensible, utilizando una terminología coherente.

24. En cuanto a los «requisitos del proceso», el Comité recomienda a la AC LU que:

    1. modifique la sección 4.4 del proyecto de requisitos a fin de incluir la obligación del organismo de certificación de garantizar que se apliquen métodos de evaluación y que dichos métodos de evaluación, descritos en el mecanismo de certificación, estén normalizados y sean de aplicación general. El organismo de certificación deberá justificar cualquier desviación de los métodos de evaluación.

    2. modifique la redacción del requisito 4.4.2 para explicitar que el organismo de certificación seguirá siendo responsable de la toma de decisiones, incluso cuando recurra a expertos externos.

    3. modifique la sección 4.8 de su proyecto de requisitos de acreditación para que el organismo de certificación haga pública la información mencionada en el punto 7.8 del anexo 1 de las Directrices.

    4. aclare en la sección 4.8 cómo se llevará a cabo el seguimiento.

    5. modifique la subsección 4.10 con el fin de especificar las normas relativas a la retirada, resolución, reducción o suspensión de la certificación.

4 OBSERVACIONES FINALES

25. Este dictamen se dirige a la autoridad de control de Luxemburgo y se hará público de conformidad con el artículo 64, apartado 5, letra b), del RGPD.

26. En virtud del artículo 64, apartados 7 y 8, del RGPD, la autoridad de control deberá comunicar por medios electrónicos a la presidenta si va a mantener o modificar su proyecto de lista en el plazo de dos semanas desde la recepción del dictamen. Dentro del mismo periodo, deberá proporcionar el proyecto de lista modificado o, cuando no tenga la intención de seguir el dictamen del Comité, deberá indicar los motivos pertinentes por los cuales no tiene intención de seguir el presente dictamen, en su totalidad o en parte.

Por el Comité Europeo de Protección de Datos

La Presidenta

(Andrea Jelinek)